# Malware Details Checklist

For each malicious file related to the incident, document the following items.

* The date and time of detection
* How the malware was detected
* The list of systems where the malware was found
* The name of the malicious file, and what directory was it present in
* What the detection mechanism determined, such as the name and family of the malicious file
* Whether a copy of the malware is preserved, either manually or through a quarantine process
* The status of the analysis. Has the malware been analyzed for network and host indicators of compromise?
* Whether the malware was submitted to third parties, either through automated process or via direct action by an employee.